

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.:	10/606,661	§	Confirmation No.:	4729
Applicant:	John Kananghinis	§		
Filed:	06/25/2003	§		
TC/A.U.:	3689	§		
Examiner:	Debra L. Antonienko	§		
Title:	METHOD OF	§		
	MODELING	§		
	FRAMEWORKS AND	§		
	ARCHITECTURE IN	§		
	SUPPORT OF A	§		
	BUSINESS	§		
Docket No.:	200901639-1	§		
	(HPC.0918US)	§		

Mail Stop Appeal Brief-Patents

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

APPEAL BRIEF PURSUANT TO 37 C.F.R § 41.37

Sir:

The final rejection of claims 1-10 and 12-21 is hereby appealed.

I. REAL PARTY IN INTEREST

The real party in interest is the Hewlett-Packard Development Company, LP. The Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 11445 Compaq Center Drive West, Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF THE CLAIMS

Claims 1-10 and 12-21 have been finally rejected and are the subject of this appeal.

Claim 11 has been cancelled.

IV. STATUS OF AMENDMENTS

An Amendment under 37 C.F.R. § 1.116 was submitted on June 24, 2010 to address a typographical error. Entry of the Amendment is appropriate since the scope of the claim has not changed.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. Note that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element. Note also that the cited passages are provided as examples, as other passages in the specification or drawings not cited may also be relevant to the corresponding claim elements.

Independent claim 1 recites a method of computer modeling integrated business and information technology frameworks and architecture in support of a business, comprising:

identifying, in a computer, manageable entities of the business and an existing information technology supported by each manageable entity (Spec., p. 3, ln. 9-12);

generating, by the computer, an overall architecture (Fig. 3:109) for the business, the overall architecture defining how the manageable entities relate to each other and to the existing information technology, wherein the overall architecture contains a plurality of components, the plurality of components including a strategic plan, a business architecture, an information architecture, an application architecture, a technology infrastructure architecture, a security architecture, and an enterprise information technology management framework (Spec., p. 3, ln. 12-26; p. 6, ln. 1-25; p. 9, ln. 7-18);

implementing, in the computer, a common language in order to articulate the overall architecture (Spec., p. 3, ln. 22-24); and

generating, by the computer, a graphical representation of the overall architecture for the business according to the common language (Spec., p. 21, ln. 26 – p. 22, ln. 2; p. 27, ln. 21-27);

determining, by the computer, information technology requirements (Fig. 2B:99) for the business in response to the existing information technology and the relationship among the manageable entities (Spec., p. 14, ln. 1-20; p. 8, ln. 16-18); and

generating, by the computer, a plan (Fig. 2B:110) for implementation and deployment of future information technology among the manageable entities based on the determined information technology requirements for display by the computer within the graphical representation of the overall architecture, the plan including a future security architecture based on the future information technology and a transition between a current security architecture and the future security architecture, wherein each of the current security architecture and future security architecture includes a corresponding set of a security objective and a mix of security measures (Spec., p. 9, ln. 23 – p. 10, ln. 2; p. 12, ln. 1-10; p. 12, ln. 25 – p. 13, ln. 6; p. 15, ln. 22-27; p. 8, ln. 31 – p. 9, ln. 6).

Independent claim 12 recites a computer readable medium including code for modeling integrated business and information technology frameworks and architecture in support of a business, the code executable on a computer to:

receive data associated with manageable entities of the business and existing information technology supported by each manageable entity (Spec., p. 3, ln. 9-12);

generate an overall architecture (Fig. 3:109) defining how manageable entities of the business relate to one another and to the existing information technology (Spec., p. 3, ln. 12-26; p. 6, ln. 1-25; p. 9, ln. 7-18), the overall architecture including:

a strategic business plan component (Fig. 3: “STRATEGIC PLAN(S)”) providing context and guidance that drive definition of business functions, processes, systems, and organization (Spec., p. 9, ln. 7-18);

a business architecture component (Fig. 3: “BUSINESS ARCHITECTURE”) reflecting what the business does in the present as well as in the future to accomplish particular business requirements (Spec., p. 9, ln. 7-18);

an information architecture component (Fig. 3: “INFORMATION ARCHITECTURE”) representing what information is to be delivered to individuals across the business;

an application architecture component (Fig. 3: “APPLICATION ARCHITECTURE”) supporting business process execution and information flow (Spec., p. 9, ln. 7-18);

a technology infrastructure architecture component (Fig. 3: “TECHNOLOGY INFRASTRUCTURE ARCHITECTURE”) supporting execution of activities and defining what information technology components are needed to enable access to information (Spec., p. 9, ln. 7-18);

a security architecture component (Fig. 3: “SECURITY ARCHITECTURE”) describing how security measures fit into the overall architecture of the business to meet security objectives of the business (Spec., p. 9, ln. 7-18);

an enterprise information technology management architecture component (Fig. 3: “ENTERPRISE IT MANAGEMENT FRAMEWORK”) dealing with business and organizational management of providing information technology services and products as well as systems, network, and element management (Spec., p. 9, ln. 7-18);

generate a plan (Fig. 3B:110) for implementation and deployment of future information technology among the manageable entities pursuant to the components of the overall architecture in response to how the manageable entities relate and to the existing information technology, the plan including a future security architecture based on the future information technology and a transition between a current security architecture and the future security architecture, wherein each of the current security architecture and future security architecture includes a corresponding set of a security objective and a mix of security measures (Spec., p. 9, ln. 23 – p. 10, ln. 2; p. 12, ln. 1-10; p. 12, ln. 25 – p. 13, ln. 6; p. 15, ln. 22-27; p. 8, ln. 31 – p. 9, ln. 6).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

- A. Claims 1-10, 20, and 21 were rejected under 35 U.S.C. § 103(a) as unpatentable over Buteau (U.S. Patent No. 6,442,557) in view of Ruffin (U.S. Patent No. 6,249,769) in view of Baudoin (U.S. Patent No. 7,290,275) and further in view of McKenna (U.S. Patent Publication No. 2004/0010772).**
- B. Claims 12-19 were rejected under 35 U.S.C. § 103(a) as unpatentable over Buteau in view of Baudoin and further in view of McKenna.**

VII. ARGUMENT

The claims do not stand or fall together. Instead, Appellant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-headings as required by 37 C.F.R. § 41.37(c)(1)(vii).

- A. Claims 1-10, 20, and 21 were rejected under 35 U.S.C. § 103(a) as unpatentable over Buteau (U.S. Patent No. 6,442,557) in view of Ruffin (U.S. Patent No. 6,249,769) in view of Baudoin (U.S. Patent No. 7,290,275) and further in view of McKenna (U.S. Patent Publication No. 2004/0010772).**

1. Claims 1-10.

It is respectfully submitted that claim 1 is non-obvious over the asserted combination of Buteau, Ruffin, Baudoin, and McKenna.

To make a determination under 35 U.S.C. § 103, several basic factual inquiries must be performed, including determining the scope and content of the prior art, and ascertaining the differences between the prior art and the claims at issue. *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 U.S.P.Q. 459 (1965). Moreover, as held by the U.S. Supreme Court, it is important to identify a reason that would have prompted a person of ordinary skill in the art to combine reference teachings in the manner that the claimed invention does. *KSR International Co. v. Teleflex, Inc.*, 127 S. Ct. 1727, 1741, 82 U.S.P.Q.2d 1385 (2007).

The Examiner conceded that Buteau (the primary reference relied upon) does not disclose the following elements of claim 1:

determining, by the computer, information technology requirements for the business in response to the existing information technology and the relationship among the manageable entities; and

generating, by the computer, a plan for implementation and deployment of future information technology among the manageable entities based on the determined information technology requirements for display by the computer within the graphical representation of the overall architecture, the plan including a future security architecture based on the future information technology and a transition between a current security architecture and the future security architecture, wherein each of the current security architecture and future security architecture includes a corresponding set of a security objective and a mix of security measures. 01/26/2010 Office Action at 5.

Instead, the Examiner relied upon the following references as purportedly disclosing the claimed features missing from Buteau: Ruffin, Baudoin, and McKenna. *Id.* at 5-6.

Buteau describes a database program that is able to allow users to input and search for how architecture changes to the enterprise affect an enterprise architecture. Buteau, 2:63-65. However, Buteau provides absolutely no hint whatsoever of generating a plan for implementation and deployment of future information technology among manageable entities of a business based on determined information technology requirements, where the plan includes a future security architecture based on the future information technology and a transition between a current security architecture and a future security architecture, where each of the current security architecture and future security architecture includes a corresponding set of a security objective and a mix of security measures.

Ruffin describes generating a formal solution proposal based on evaluating an information technology environment and requirements of a business entity (Ruffin, Abstract). However, Ruffin does not provide any hint that the formal solution proposal would include a plan that includes a future security architecture based on the future information technology and a

transition between a current security architecture and the future security architecture, as defined by claim 1. Although Ruffin notes that its techniques can be applied to plant security (*id.*, 3:16), there is no hint that the techniques of Ruffin would produce a plan as defined by claim 1.

Recognizing the deficiencies of Buteau and Ruffin, the Examiner cited the teachings of Baudoin and McKenna. Specifically, the Examiner cited the Abstract, Fig. 4, and column 51, line 50 – column 52, line 57, of Baudoin, and the following passages of McKenna: ¶¶ [0082]-[0084]. The Abstract of Baudoin notes that an information security policy and practice of an organization are assessed, which includes determining a risk associated with the information security policy and practice. The Abstract of Baudoin also notes that a rating is generated using a security maturity assessment matrix. The Abstract of Baudoin also notes that a list of corrective actions is generated using the rating. The list of corrective actions is executed to create a new security information policy and practice.

The passage at column 51, line 50 – column 52, line 57, of Baudoin refers to generating a corrective action plan (CAP). This passage notes that proposed actions are aimed at improving the items that have gaps the bringing the items up to the goal. Baudoin, 51:52-55. The passage also refers to a monitoring phase to ensure that goals are met and maintained. *Id.*, 51:64-65. During the monitoring phase, an assessment entity can detect a change in the environment that may require additions or changes to the security practices and/or policies. *Id.*, 51:66-52:1. Baudoin also discloses determining an organization's business goals, as well as the associated risk in terms of information security. *Id.*, 52:7-11. Written documentation is collected about the organization's existing information security policies and practices. *Id.*, 52:11-13. Additional information is then collected via interviews. *Id.*, 52:13-14. Using the information gathered, a security assessment matrix rating is generated. *Id.*, 52:14-16. A list of corrective actions is then

proposed, and the actions are subsequently prioritized and executed to generate modified information security policies. *Id.*, 52:17-21.

Significantly, note that the passage in columns 51 and 52 cited by the Examiner teaches a modification of an organization's existing information security policies and practices based on information gathered regarding the existing infrastructure, in the form of the existing information security policies and practices and other gathered information. However, generating modifications to information security policies and practices in the form of the corrective actions discussed in Baudoin is different from generating a plan including a future security architecture based on the future information technology and a **transition** between a current security architecture and the future security architecture, where **each of the current security architecture and future security architecture** includes a corresponding set of a security objective and a mix of security measures.

In Baudoin, existing information security policies and practices are modified based on interviews and written documentation collected about the existing information security policies and practices. According to Baudoin, corrective actions are listed based on the existing information security policies and practices and interview information. The corrective actions are then executed to generate modified information security policies and procedures. This type of modification of security policies and practices does not constitute generating a plan as specifically defined by claim 1, which includes both the future security architecture based on the future information technology and the transition between the current security architecture and the future security architecture, where each of the current and future security architectures includes a corresponding set of a security objective and a mix of security measures.

The Examiner apparently recognized the deficiency of Baudoin, but instead, argued that “[s]etting objectives and determining measures to achieve the objectives are old and well-known for an enterprise.” 01/26/2010 Office Action at 6. As purported support for this allegation, the Examiner cited column 5, line 21 – column 6, line 48, of Buteau. This passage of Buteau refers to a framework for an enterprise architecture database that has been developed to meet several objectives. Buteau, 5:33-34. Among the objectives are provision for the representation of planned or possible future architectures and to extend to encompass alternative or future perspectives on technologies. *Id.*, 5:38-43. However, even though Buteau refers to a framework for an enterprise architecture database to meet various objectives as noted, it is clear that Buteau provides no hint of the generated plan of claim 1, which includes both a future security architecture based on the future information technology and a transition between the current security architecture and the future security architecture, where each of the current security architecture and future security architecture includes a corresponding set of a security objective and a mix of security measures. Moreover, it is noted that Baudoin teaches a technique for modifying existing information security policies and practices in a manner that is quite different from the technique recited in claim 1. A person of ordinary skill in the art would not have been prompted to apply the teachings of Buteau regarding its framework to the security policies/practices modification technique of Baudoin.

It is also apparent that the Examiner conceded that Baudoin and Buteau still do not disclose or hint at the plan that includes the transition between the current and future security architectures as claimed. Instead, the Examiner cited McKenna as disclosing a plan to transition from a present system to a new system. 01/26/2010 Office Action at 6. Specifically, the Examiner cited ¶¶ [0082]-[0084] of McKenna, which describe establishing an organization plan

for managing resources for a project. Note that the project discussed by McKenna is a project for developing and implementing new computer software applications through a series of distinct stages. McKenna, Abstract. In McKenna, a user process narrative sign-off, an application set of configurations sign-off, a design securities profiles sign-off, and a design acceptance certificate are each provided to ensure that adequate and accurate information regarding the design of the software being developed are provided prior to review. These teachings of McKenna have nothing to do with generating a plan that includes a future security architecture based on the future information technology and a transition between a current security architecture and the future security architecture, where each of the current security architecture and future security architecture includes a corresponding set of a security objective and a mix of security measures.

Although ¶ [0082] of McKenna refers to a plan to transition from a present system to a new system, there is no hint in McKenna that the plan of McKenna includes the transition between the current security architecture and the future security architecture, where each of the current and future security architectures includes a corresponding set of a security objective and a mix of security measures. Paragraph [0083] of McKenna refers to a design security profiles sign-off 856—there is no hint that such design security profiles sign-off 856 includes the transition between the current and future security architecture where each of the current and future security architectures includes a corresponding set of a security objective and a mix of security measures.

Paragraph [0084] of McKenna states that various associated sign-offs are provided to support the development of the enterprise architecture, including a design of a security architecture sign-off, a design application functional architecture sign-off, a developed system capacity plan sign-off, an assess performance risks sign-off, and a design system management

sign-off, which are provided to ensure that proper development and documentation of each of the items has been performed prior to approval. Again, except for the common use of the term “security,” McKenna in ¶ [0084] provides absolutely no hint of the plan that includes a future security architecture based on the future information technology and a transition between a current security architecture and the future security architecture, as recited in claim 1.

In view of the foregoing, it is respectfully submitted that even if the references could be hypothetically combined, Buteau, Ruffin, Baudoin, and McKenna would not disclose or hint at all elements of claim 1. Moreover, in view of the fact that none of the references provide any hint of the subject matter in the last clause of claim 1 (the “generate” clause), it is respectfully submitted that a person of ordinary skill in the art would not have been prompted to combine the teachings of the references to achieve the claimed subject matter.

Therefore, the obviousness rejection of claim 1 and its dependent claims is erroneous.

Reversal of the final rejection of the above claims is respectfully requested.

2. Claim 20.

Claim 20 depends from claim 1 and is therefore allowable for at least the same reasons as claim 1. Moreover, claim 20 further recites:

analyzing industry benchmarks relating to information technology practices, wherein generating the plan is further based on analyzing the industry benchmarks relating to information technology practices.

As purportedly disclosing the foregoing subject matter of claim 20, the Examiner cited Ruffin, column 18, line 29 – column 19, line 31, and column 52, lines 54-57, of Baudoin. With respect to Ruffin, the Examiner focused on the following statement made in Ruffin:

An excellent source of this and other benchmark which are well known to those skilled in the art may currently be found on the Internet's World Wide Web at the universal resource locator (URL): ... presented by Ideas International Corporation.

Ruffin, 19:6-11. The noted benchmark is used for determining the transactions per minute (Tpm) rating for a particular workload. *Id.*, 19:1-3. The Tpm represents a machine capacity. As further noted in the cited passage of Ruffin, for an entered workload type, it is determined whether a workload benchmark for determining the requisite machine capacity is known for the particular workload. *Id.*, 18:65-66. Thus, the benchmark of Ruffin is used for determining a machine capacity for a particular workload. Using the benchmark in this way has nothing to do with the subject matter of claim 20, which relates to analyzing industry benchmarks relating to information technology practices, where **generating the plan** is further **based on analyzing the industry benchmarks relating to information technology practices**. There is absolutely no hint whatsoever in Ruffin that its benchmark is analyzed for generating the plan recited in base claim 1, where the plan includes the transition between current and future security architectures each including a corresponding set of a security objective and a mix of security measures.

Baudoin in column 52, lines 54-57, states that its security assessment matrix (SMA) can be used for the purpose of meeting a certain industry standard or reaching a goal established through analysis of the competition's security capabilities. Thus, it appears that the Examiner is equating "industry standard" in this passage of Baudoin with the "industry benchmarks" recited in claim 20. However, there is no hint in Baudoin of generating the plan recited in base claim 1 based on analyzing the industry benchmarks relating to information technology practices.

Therefore, it is respectfully submitted that claim 20 is further allowable over the cited references for the foregoing reasons.

Reversal of the final rejection of the above claim is respectfully requested.

3. Claims 21.

Claim 21 depends from claim 12, and recites similar subject matter as claim 20. Claim 21 is further allowable for similar reasons as stated above with respect to claim 20.

Reversal of the final rejection of the above claims is respectfully requested.

B. Claims 12-19 were rejected under 35 U.S.C. § 103(a) as unpatentable over Buteau in view of Baudoin and further in view of McKenna.

1. Claims 12-19.

Independent claim 12 was rejected as purportedly obvious over Buteau, Baudoin, and McKenna. The rejection of claim 12 left off Ruffin as a reference. With respect to claim 12, the Examiner conceded that Buteau fails to disclose the plan that is generated according to claim 12. 01/26/2010 Office Action at 8. The “plan” of claim 12 is defined in the following clause of claim 12:

generate a plan for implementation and deployment of future information technology among the manageable entities pursuant to the components of the overall architecture in response to how the manageable entities relate and to the existing information technology, the plan including a future security architecture based on the future information technology and a transition between a current security architecture and the future security architecture, wherein each of the current security architecture and future security architecture includes a corresponding set of a security objective and a mix of security measures.

As purportedly disclosing the foregoing subject matter of claim 12, the Examiner cited Baudoin and McKenna. The passages of Baudoin and McKenna cited by the Examiner against the “generate” element of claim 12 are the same passages cited against the “generating” element of claim 1. As discussed above in connection with claim 1, it is clear that Baudoin and McKenna clearly do not provide any teaching or hint of the foregoing claimed subject matter. Specifically, Baudoin and McKenna do not provide any hint of a plan including a future security architecture based on the future information technology and a transition between the current and future

security architectures, where **each** of the current and future security architectures includes a corresponding set of a security objective and a mix of security measures.

Thus, even if Buteau, Baudoin, and McKenna could be hypothetically combined, the hypothetical combination of the references would not have led to the subject matter of claim 12. Moreover, in view of the significant differences between the claimed subject matter and the teachings of the cited references, a person of ordinary skill in the art would not have been prompted to combine the teachings of the references to achieve the claimed subject matter.

Therefore, the obviousness rejection of claim 12 and its dependent claims is clearly erroneous.

Reversal of the final rejection of the above claims is respectfully requested.

CONCLUSION

In view of the foregoing, reversal of all final rejections and allowance of all pending claims is respectfully requested.

Respectfully submitted,

Date: June 25, 2010

/Dan C. Hu/

Dan C. Hu
Registration No. 40,025
TROP, PRUNER & HU, P.C.
1616 South Voss Road, Suite 750
Houston, TX 77057-2631
Telephone: (713) 468-8880
Facsimile: (713) 468-8883

VIII. APPENDIX OF APPEALED CLAIMS

Claim 11 has been cancelled.

The claims on appeal are:

1. A method of computer modeling integrated business and information technology frameworks and architecture in support of a business, comprising:

- identifying, in a computer, manageable entities of the business and an existing information technology supported by each manageable entity;
- generating, by the computer, an overall architecture for the business, the overall architecture defining how the manageable entities relate to each other and to the existing information technology, wherein the overall architecture contains a plurality of components, the plurality of components including a strategic plan, a business architecture, an information architecture, an application architecture, a technology infrastructure architecture, a security architecture, and an enterprise information technology management framework;
- implementing, in the computer, a common language in order to articulate the overall architecture; and
- generating, by the computer, a graphical representation of the overall architecture for the business according to the common language;
- determining, by the computer, information technology requirements for the business in response to the existing information technology and the relationship among the manageable entities; and
- generating, by the computer, a plan for implementation and deployment of future information technology among the manageable entities based on the determined information technology requirements for display by the computer within the graphical representation of the overall architecture, the plan including a future security architecture based on the future information technology and a transition between a current security architecture and the future security architecture, wherein each of the current security architecture and future security architecture includes a corresponding set of a security objective and a mix of security measures.

1 2. The method of Claim 1, wherein the overall architecture addresses people,
2 processes, and technology of the business.

1 3. The method of Claim 1, wherein the strategic plan component includes a business
2 plan, a product plan, a financial plan, an organization plan, a marketing plan, and a future
3 information technology plan in support of the aforementioned plans.

1 4. The method of Claim 1, wherein the business architecture component defines
2 current business direction, objectives, and supporting processes as well as future direction,
3 objectives, and supporting processes.

1 5. The method of Claim 1, wherein the information architecture component provides
2 information and data management precepts, an information-application software portfolio, and a
3 geo-structural view of existing and future information technology deployment.

1 6. The method of Claim 1, wherein the application architecture component defines
2 an application software portfolio and integration relationships for the manageable entities of the
3 business.

1 7. The method of Claim 1, wherein the technology infrastructure architecture
2 component enables access to information and geo-structural layouts for the existing and future
3 information technology.

1 8. The method of Claim 1, wherein the security architecture component describes
2 how security measures fit into the overall architecture of the business to meet security objectives
3 of the business.

1 9. The method of claim 1, wherein the enterprise information technology
2 management framework component provides existing and future information technology
3 services and products, management of the services, information technology systems and network
4 management, and enterprise information technology management organization capabilities,
5 competencies, skills, and performance models.

1 10. The method of Claim 1, further comprising:
2 decomposing, by the computer, the manageable entities so that each manageable entity
3 has a relative independence from other manageable entities but is in context with the overall
4 enterprise architecture.

1 12. A computer readable medium including code for modeling integrated business
2 and information technology frameworks and architecture in support of a business, the code
3 executable on a computer to:

4 receive data associated with manageable entities of the business and existing information
5 technology supported by each manageable entity;

6 generate an overall architecture defining how manageable entities of the business relate to
7 one another and to the existing information technology, the overall architecture including:

8 a strategic business plan component providing context and guidance that drive
9 definition of business functions, processes, systems, and organization;

10 a business architecture component reflecting what the business does in the present
11 as well as in the future to accomplish particular business requirements;

12 an information architecture component representing what information is to be
13 delivered to individuals across the business;

14 an application architecture component supporting business process execution and
15 information flow;

16 a technology infrastructure architecture component supporting execution of
17 activities and defining what information technology components are needed to enable access to
18 information;

19 a security architecture component describing how security measures fit into the
20 overall architecture of the business to meet security objectives of the business;

21 an enterprise information technology management architecture component
22 dealing with business and organizational management of providing information technology
23 services and products as well as systems, network, and element management;

24 generate a plan for implementation and deployment of future information technology
25 among the manageable entities pursuant to the components of the overall architecture in response
26 to how the manageable entities relate and to the existing information technology, the plan
27 including a future security architecture based on the future information technology and a
28 transition between a current security architecture and the future security architecture, wherein
29 each of the current security architecture and future security architecture includes a corresponding
30 set of a security objective and a mix of security measures.

1 13. The computer readable medium of Claim 12, wherein the security architecture
2 component includes security and business continuity requirements, an information security view,
3 an application security view, a security infrastructure view, and an information security
4 administration/management/training view.

1 14. The computer readable medium of Claim 13, wherein the information security
2 view is responsible for supervision of data within the overall architecture of the business.

1 15. The computer readable medium of Claim 13, wherein the application security
2 view is responsible for the supervision of applications within the overall structure of the
3 business.

1 16. The computer readable medium of Claim 13, wherein the security infrastructure
2 view is responsible for supervision of an infrastructure within the overall architecture of the
3 business.

1 17. The computer readable medium of Claim 13, wherein the information security
2 administration/management/training view is responsible for managing access and recovery of
3 data within the overall architecture of the business.

1 18. The computer readable medium of Claim 13, wherein the security and business
2 continuity requirements provide inputs for implementing information security within the overall
3 architecture of the business.

1 19. The computer readable medium of Claim 13, wherein the code is further
2 executable to:

3 graphically displaying the overall architecture of the business;

4 graphically displaying how the future information technology is to be implemented and
5 deployed within the overall architecture in response to the generated plan.

1 20. The method of claim 1, further comprising:
2 analyzing industry benchmarks relating to information technology practices, wherein
3 generating the plan is further based on analyzing the industry benchmarks relating to information
4 technology practices.

1 21. The computer readable media of claim 12, wherein the code is executable to
2 further:
3 analyze industry benchmarks relating to information technology practices, wherein
4 generating the plan is further based on analyzing the industry benchmarks relating to information
5 technology practices.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.